

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-040172

(43)Date of publication of application : 13.02.1998

(51)Int.Cl. G06F 12/14
H04L 9/08

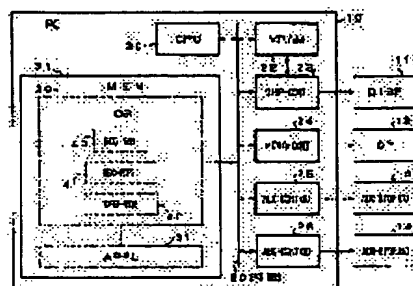
(21)Application number : 08-196202 (71)Applicant : TOSHIBA CORP

(22)Date of filing : 25.07.1996 (72)Inventor : OKA HIROYUKI

(54) COMPUTER SYSTEM AND DATA TRANSFER METHOD**(57)Abstract:**

PROBLEM TO BE SOLVED: To protect data whose copy is restricted on the same computer system by providing a function for ciphering by using a public key cryptosystem for data transferred between a processor and an auxiliary storage device in the computer system.

SOLUTION: The auxiliary storage device 13 acquires a secret key 40 which is needed to cipher data by using the public key cryptosystem from an operating system 30, uses the secret key 40 to cipher the data, and reports the ciphering at the transfer of the ciphered data. The operating system 30 generates the secret key 40 need for the ciphering, ciphers this secret key 30 by using a public key obtained from the auxiliary storage device 13, and then sends it to the auxiliary device 13; when the ciphering is reported at the transfer of data from the auxiliary storage device 13, the ciphered data are deciphered and sent to an output signal process routine 42 in the operating system 30.

**LEGAL STATUS**

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2000 Japanese Patent Office

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平10-40172

(43) 公開日 平成10年(1998) 2月13日

(51) IntCl.⁶

G 0 6 F 12/14

H 0 4 L 9/08

識別記号

3 2 0

庁内整理番号

F I

G 0 6 F 12/14

H 0 4 L 9/00

技術表示箇所

3 2 0 B

6 0 1 A

6 0 1 C

6 0 1 E

審査請求 未請求 請求項の数15 O L (全 15 頁)

(21) 出願番号

特願平8-196202

(22) 出願日

平成8年(1996) 7月25日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 岡 弘幸

東京都青梅市末広町2丁目9番地 株式会

社東芝青梅工場内

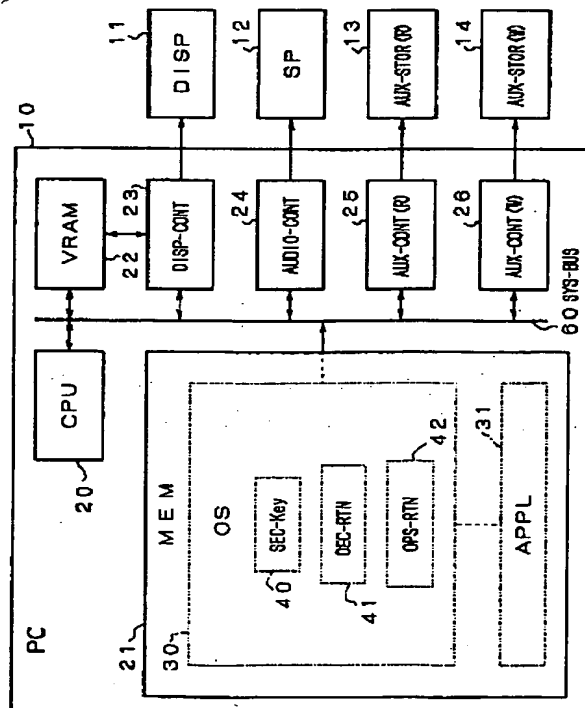
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 コンピュータシステム及びデータ転送方法

(57) 【要約】

【課題】本発明は、コンピュータシステム上の処理装置と補助記憶装置との間で受け渡されるデータに公開鍵暗号化方式を用いて暗号化を施す機能を設けて、製を規制するデータの保護を同一コンピュータシステム上に於いても行なう。

【解決手段】補助記憶装置13は、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵40をオペレーティングシステム30から取得し、その秘密鍵40を用いてデータを暗号化し、暗号化したデータの転送時には暗号化したことを知らせる。オペレーティングシステム30は、暗号化に必要な秘密鍵40を生成し、補助記憶装置13から得た公開鍵を用いて、この秘密鍵40を暗号化した後、補助記憶装置13に送り、補助記憶装置13からのデータの転送時に暗号化されたことを知らされた場合には、オペレーティングシステム30内部の出力信号処理ルーチン42に対しては暗号化されたデータを復号化して送る。



【特許請求の範囲】

【請求項1】 バスを介して処理装置と補助記憶装置との間でデータが受け渡されるコンピュータシステムに於いて、

前記補助記憶装置に、

公開鍵となる暗号化用の鍵及び復号化用の鍵を生成する手段と、

前記処理装置よりデータを暗号化するための秘密鍵を取得する際に、前記暗号化用の鍵を前記処理装置に転送する手段と、

前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受けたとき、当該秘密鍵を前記復号化用の鍵を用いて復号化処理して前記処理装置で生成した秘密鍵を取得する手段と、

前記処理装置へ転送するデータを前記取得した秘密鍵を用いて暗号化処理し、秘密鍵を用いて暗号化したことを通知する信号とともに前記処理装置へ転送する手段とを有し、

前記処理装置に、

データの暗号化に必要な秘密鍵を生成する手段と、

前記補助記憶装置より前記暗号化用の鍵を受け取ったとき、当該暗号化用の鍵を用いて前記内部で生成した秘密鍵を暗号化処理した後、前記補助記憶装置に転送する手段と、

前記補助記憶装置より秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記補助記憶装置より受けたデータを前記内部で生成した秘密鍵を用いて復号化処理する手段とを有して、

システム内でバスを介して受け渡される補助記憶装置の読出データに秘密鍵を用いて暗号化処理を施すことを特徴としたコンピュータシステム。

【請求項2】 バスを介して処理装置と補助記憶装置との間でデータが受け渡されるコンピュータシステムに於いて、

前記補助記憶装置に、

公開鍵となる暗号化用の鍵及び復号化用の鍵を生成する手段と、

前記処理装置よりデータを復号化するための秘密鍵を取得する際に、前記暗号化用の鍵を前記処理装置に転送する手段と、

前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、

前記処理装置より秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記処理装置より転送された書き込みデータを前記秘密鍵を用いて復号化処理した後、記憶媒体に書き込む手段とを有し、

前記処理装置に、

秘密鍵を生成する手段と、

前記補助記憶装置より前記暗号化用の鍵を受け取ったとき、前記内部で生成した秘密鍵を前記補助記憶装置より受け取った暗号化用の鍵を用いて暗号化し、前記補助記憶装置に転送する手段と、

前記補助記憶装置の記憶媒体に書き込むデータに前記内部で生成した秘密鍵を用いて暗号化処理を施し、当該データを秘密鍵を用いて暗号化したことを通知する信号とともに前記補助記憶装置に転送する手段とを有して、システム内でバスを介して受け渡される補助記憶装置の書き込みデータに秘密鍵を用いて暗号化処理を施すことを特徴としたコンピュータシステム。

【請求項3】 処理装置と、記憶媒体に記憶されたデータを読出す第1の補助記憶手段と、記憶媒体にデータを書込む第2の補助記憶手段とをもつコンピュータシステムに於いて、

前記処理装置は、

秘密鍵を生成する手段と、

前記第1又は第2の補助記憶手段より暗号化用の公開鍵を受け取ったとき、当該公開鍵を用いて前記内部で生成した秘密鍵を暗号化し、前記公開鍵を発送した補助記憶手段に転送する手段とを有し、

前記第1の補助記憶手段は、

暗号化用及び復号化用の公開鍵を生成する手段と、

前記処理装置より秘密鍵を取得する際に、前記暗号化用の公開鍵を前記処理装置に転送する手段と、

前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の公開鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、

前記処理装置へ転送するデータを前記取得した秘密鍵を用いて暗号化処理し、秘密鍵を用いて暗号化したことを通知する信号とともに前記処理装置を介して前記第2の補助記憶手段へ転送する手段とを有し、

前記第2の補助記憶手段は、

暗号化用及び復号化用の公開鍵を生成する手段と、

前記処理装置より秘密鍵を取得する際に、前記暗号化用の公開鍵を前記処理装置に転送する手段と、

前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の公開鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、

前記秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記第1の補助記憶手段より転送されたデータを前記取得した秘密鍵を用いて復号化処理した後、記憶媒体に書き込む手段とを有し、

システム内で受け渡される補助記憶データを秘密鍵を用いて暗号化処理することを特徴としたコンピュータシステム。

【請求項4】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに

於いて、

公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を処理装置のオペレーティングシステムから取得し当該秘密鍵を用いてデータを暗号化する手段と、前記秘密鍵を用いて暗号化した転送データを当該転送データが暗号化される信号とともに処理装置に転送する手段とをもつ補助記憶装置と、

暗号化に必要な秘密鍵を生成する手段と、前記生成した秘密鍵を前記補助記憶装置から取得した公開鍵を用いて暗号化し前記補助記憶装置に転送する手段と、前記補助記憶装置から転送されるデータが暗号化されている旨の通知を受けたとき、内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化し、それ以外のルーチンに対しては転送データが暗号化されていることを通知する手段と、データの復号化に必要な秘密鍵を公開鍵暗号方式を用いて送出する手段とをもつ処理装置のオペレーティングシステムとを具備してなることを特徴とするコンピュータシステム。

【請求項5】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、

公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を処理装置のオペレーティングシステムから取得し当該秘密鍵を用いてデータを暗号化する手段と、前記秘密鍵を用いて暗号化した転送データを当該転送データが暗号化されていることを通知する信号とともに処理装置に転送する手段とをもつ第1の補助記憶手段と、暗号化されたデータの記録時に公開鍵暗号方式を用いて受け取った秘密鍵によりデータの復号化を行なった後、記録メディアに記録する手段をもつ第2の補助記憶手段と、

暗号化に必要な秘密鍵を生成する手段と、前記生成した秘密鍵を前記第1又は第2の補助記憶手段から取得した公開鍵を用いて暗号化し前記第1又は第2の補助記憶手段に転送する手段と、前記第1の補助記憶手段から転送されるデータが暗号化されている旨の通知を受けたとき、内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化し、それ以外のルーチン及び前記第2の補助記憶手段に対しては転送されるデータが暗号化されていることを通知する手段と、データの復号化に必要な秘密鍵を公開鍵暗号方式を用いて送出する手段とをもつ処理装置のオペレーティングシステムとを具備してなることを特徴とするコンピュータシステム。

【請求項6】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、

公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが

可能で、暗号化したデータの転送時に暗号化レベルを知らせることが可能な補助記憶装置と、

暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記補助記憶装置から得た公開鍵を用いて前記生成した秘密鍵を暗号化した後、前記補助記憶装置に送ることができ、前記補助記憶装置からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチンに対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴としたコンピュータシステム。

【請求項7】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、

公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時には暗号化レベルを知らせることが可能な第1の補助記憶手段と、暗号化されたデータの記録時には公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じたデータの復号化を行ない、当該データを記録メディアに記録することが可能な第2の補助記憶手段と、

暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記第1又は第2の補助記憶手段から得た公開鍵を用いて前記生成した秘密鍵を暗号化した後、前記第1又は第2の補助記憶手段に送ることができ、前記第1の補助記憶手段からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチン及び前記第2の補助記憶手段に対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴としたコンピュータシステム。

【請求項8】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、

公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時に暗号化レベルを知らせることが可能な補助記憶装置と、

暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記補助記憶装置から得た公開鍵を用いて当該秘密鍵を暗号化した後、前記補助記憶装置に送ることができ、前記

補助記憶装置からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチンに対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴としたコンピュータシステム。

【請求項 9】 処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、

公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時には暗号化レベルを知らせることが可能な第 1 の補助記憶手段と、

暗号化されたデータの記録時には公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じたデータの復号化を行ない、当該データを記録メディアに記録することが可能な第 2 の補助記憶手段と、

暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記第 1 又は第 2 の補助記憶手段から得た公開鍵を用いて当該秘密鍵を暗号化した後、前記第 1 又は第 2 の補助記憶手段に送ることができ、前記第 1 の補助記憶手段からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチン及び前記第 2 の補助記憶手段に対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴としたコンピュータシステム。

【請求項 10】 システム内でバスを經由して受け渡される動画データに秘密鍵を用いて暗号化処理を施す請求項 1 又は 2 又は 3 又は 4 又は 5 又は 6 又は 7 又は 8 又は 9 記載のコンピュータシステム。

【請求項 11】 システム内でバスを經由して受け渡される圧縮化された動画データに秘密鍵を用いて暗号化処理を施す請求項 1 又は 2 又は 3 又は 4 又は 5 又は 6 又は 7 又は 8 又は 9 記載のコンピュータシステム。

【請求項 12】 第 1 の補助記憶手段と第 2 の補助記憶手段はそれぞれ独立したディスクドライブ機構をもつ記憶装置により実現される請求項 3 又は 5 又は 7 又は 9 記載のコンピュータシステム。

【請求項 13】 第 1 の補助記憶手段と第 2 の補助記憶手段は単一の大容量記憶装置により実現される請求項 3 又は 5 又は 7 又は 9 記載のコンピュータシステム。

【請求項 14】 システム内でバスを經由して受け渡される動画データに公開鍵暗号方式による秘密鍵を用いて

暗号化処理を施すコンピュータシステムのデータ転送方法。

【請求項 15】 システム内でバスを經由して受け渡される圧縮化された動画データに公開鍵暗号方式による秘密鍵を用いて暗号化処理を施すコンピュータシステムのデータ転送方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、コンピュータシステム上で著作権保護を必要とするデータ扱う際に適用して好適なコンピュータシステムに関する。又、本発明は、補助記憶装置内のデータの暗号化及び暗号化データの扱いを考慮したコンピュータシステムに関する。

【0002】又、本発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに関する。又、本発明は、バスを經由して動画データが受け渡されるコンピュータシステムのデータ転送方法に関する。

【0003】

【従来の技術】従来、コンピュータ上に於ける著作権保護を必要とするデータの扱いに関しては、データ中に複製禁止を示すフラグを立てるなどの方法が採られてきた。また、コンピュータ間の通信に於いては、通信相手を特定するための認証機構や転送されたデータを第三者から保護するための守秘機構など利用目的に応じて様々な方式が考えられている。

【0004】しかしながら上記した各セキュリティ技術はいずれも通信手段を介してやり取りされる情報を対象としたものであり、コンピュータシステムの内部に於ける補助記憶装置とオペレーティングシステムとの間の暗号化による有効なデータセキュリティ技術に関しては何等の考慮もなされていなかった。

【0005】また、伝送経路上に於ける暗号化されたデータの扱いについては様々な方式が考えられているが、コンピュータの主メモリに記憶するデータに対して暗号化を考慮したものは存在しなかった。このため、従来では同一コンピュータ上に於いて複製を規制するデータを確実に保護することが困難であった。

【0006】

【発明が解決しようとする課題】上記したように、従来、データの暗号化方式に関しては、いくつかの方法が考えられてきたが、コンピュータシステム上に於ける補助記憶装置とオペレーティングシステムとの間の暗号化による有効なデータセキュリティ技術がなく、また、伝送経路上に於ける暗号化されたデータの扱いについても様々な方式が考えられているが、コンピュータの主メモリに記憶するデータに対して暗号化を考慮したものは存在しなかった。従って従来では同一コンピュータ上に於いて複製を規制するデータを確実に保護することができないという問題があった。

【0007】本発明は上記実情に鑑みなされたもので、コンピュータシステム上に於ける補助記憶装置とオペレーティングシステムとの間に於ける転送データについても有効な暗号化処理を施し複製を確実に防止して信頼性の高いデータ保護機能を実現できる補助記憶装置内のデータの暗号化及び暗号化データの扱いを考慮したコンピュータシステムを提供することを目的とする。

【0008】又、本発明は、コンピュータシステム内でバスを経由して受け渡される動画データの複製を確実に防止して信頼性の高いデータ保護機能を実現できるコンピュータシステム及びコンピュータシステムのデータ転送方法を提供することを目的とする。

【0009】

【課題を解決するための手段】本発明は、コンピュータシステム上に於いて、処理装置と補助記憶装置との間で受け渡されるデータに公開鍵暗号化方式を用いて暗号化を施す機能を設けて、動画データ等、複製を規制するデータの保護を同一コンピュータシステム上に於いても行なうようにしたことを特徴とする。

【0010】又、本発明は、システム内でバスを経由して受け渡されるデータに公開鍵暗号方式による秘密鍵を用い暗号化処理を施す機能を設けて、動画データ等、複製を規制するデータの保護を同一コンピュータシステム上に於いても行なうようにしたことを特徴とする。

【0011】即ち、第1の発明は、バスを介して処理装置と補助記憶装置との間でデータが受け渡されるコンピュータシステムに於いて、前記補助記憶装置に、公開鍵となる暗号化用の鍵及び復号化用の鍵を生成する手段と、前記処理装置よりデータを暗号化するための秘密鍵を取得する際に、前記暗号化用の鍵を前記処理装置に転送する手段と、前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受けたとき、当該秘密鍵を前記復号化用の鍵を用い復号化処理して前記処理装置で生成した秘密鍵を取得する手段と、前記処理装置へ転送するデータを前記取得した秘密鍵を用いて暗号化処理し、秘密鍵を用いて暗号化したことを通知する信号とともに前記処理装置へ転送する手段とを有し、前記処理装置に、データの暗号化に必要な秘密鍵を生成する手段と、前記補助記憶装置より前記暗号化用の鍵を受け取ったとき、当該暗号化用の鍵を用いて前記内部で生成した秘密鍵を暗号化処理した後、前記補助記憶装置に転送する手段と、前記補助記憶装置より秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記補助記憶装置より受けたデータを前記内部で生成した秘密鍵を用いて復号化処理する手段とを有して、システム内でバスを介して受け渡される補助記憶装置の読出データに秘密鍵を用いて暗号化処理を施すことを特徴とする。

【0012】又、第2の発明は、バスを介して処理装置と補助記憶装置との間でデータが受け渡されるコンピュータシステムに於いて、前記補助記憶装置に、公開鍵と

なる暗号化用の鍵及び復号化用の鍵を生成する手段と、前記処理装置よりデータを復号化するための秘密鍵を取得する際に、前記暗号化用の鍵を前記処理装置に転送する手段と、前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、前記処理装置より秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記処理装置より転送された書き込みデータを前記秘密鍵を用いて復号化処理した後、記憶媒体に書き込む手段とを有し、前記処理装置に、秘密鍵を生成する手段と、前記補助記憶装置より前記暗号化用の鍵を受け取ったとき、前記内部で生成した秘密鍵を前記補助記憶装置より受け取った暗号化用の鍵を用いて暗号化し、前記補助記憶装置に転送する手段と、前記補助記憶装置の記憶媒体に書き込むデータに前記内部で生成した秘密鍵を用いて暗号化処理を施し、当該データを秘密鍵を用いて暗号化したことを通知する信号とともに前記補助記憶装置に転送する手段とを有して、システム内でバスを介して受け渡される補助記憶装置の書き込みデータに秘密鍵を用いて暗号化処理を施すことを特徴とする。

【0013】又、第3の発明は、処理装置と、記憶媒体に記憶されたデータを読出す第1の補助記憶手段と、記憶媒体にデータを書込む第2の補助記憶手段とをもつコンピュータシステムに於いて、前記処理装置は、秘密鍵を生成する手段と、前記第1又は第2の補助記憶手段より暗号化用の公開鍵を受け取ったとき、当該公開鍵を用いて前記内部で生成した秘密鍵を暗号化し、前記公開鍵を発送した補助記憶手段に転送する手段とを有し、前記第1の補助記憶手段は、暗号化用及び復号化用の公開鍵を生成する手段と、前記処理装置より秘密鍵を取得する際に、前記暗号化用の公開鍵を前記処理装置に転送する手段と、前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の公開鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、前記処理装置へ転送するデータを前記取得した秘密鍵を用いて暗号化処理し、秘密鍵を用いて暗号化したことを通知する信号とともに前記処理装置を介して前記第2の補助記憶手段へ転送する手段とを有し、前記第2の補助記憶手段は、暗号化用及び復号化用の公開鍵を生成する手段と、前記処理装置より秘密鍵を取得する際に、前記暗号化用の公開鍵を前記処理装置に転送する手段と、前記処理装置より前記暗号化用の鍵により暗号化された秘密鍵を受け取ったとき、当該秘密鍵を前記復号化用の公開鍵により復号化して前記処理装置で生成した秘密鍵を取得する手段と、前記秘密鍵を用いて暗号化したことを通知する信号を受けたとき、前記第1の補助記憶手段より転送されたデータを前記取得した秘密鍵を用いて復号化処理した後、記憶媒体に書き込む手段とを有し、システム内で受け渡される補

助記憶データを秘密鍵を用いて暗号化処理することを特徴とする。

【0014】又、第4の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を処理装置のオペレーティングシステムから取得し当該秘密鍵を用いてデータを暗号化する手段と、前記秘密鍵を用いて暗号化した転送データを当該転送データが暗号化される信号とともに処理装置に転送する手段とをもつ補助記憶装置と、暗号化に必要な秘密鍵を生成する手段と、前記生成した秘密鍵を前記補助記憶装置から取得した公開鍵を用いて暗号化し前記補助記憶装置に転送する手段と、前記補助記憶装置から転送されるデータが暗号化されている旨の通知を受けたとき、内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化し、それ以外のルーチンに対しては転送データが暗号化されていることを通知する手段と、データの復号化に必要な秘密鍵を公開鍵暗号方式を用いて送出する手段とをもつ処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0015】又、第5の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を処理装置のオペレーティングシステムから取得し当該秘密鍵を用いてデータを暗号化する手段と、前記秘密鍵を用いて暗号化した転送データを当該転送データが暗号化されていることを通知する信号とともに処理装置に転送する手段とをもつ第1の補助記憶手段と、暗号化されたデータの記録時に公開鍵暗号方式を用いて受け取った秘密鍵によりデータの復号化を行なった後、記録メディアに記録する手段をもつ第2の補助記憶手段と、暗号化に必要な秘密鍵を生成する手段と、前記生成した秘密鍵を前記第1又は第2の補助記憶手段から取得した公開鍵を用いて暗号化し前記第1又は第2の補助記憶手段に転送する手段と、前記第1の補助記憶手段から転送されるデータが暗号化されている旨の通知を受けたとき、内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化し、それ以外のルーチン及び前記第2の補助記憶手段に対しては転送されるデータが暗号化されていることを通知する手段と、データの復号化に必要な秘密鍵を公開鍵暗号方式を用いて送出する手段とをもつ処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0016】上記したコンピュータシステムに於いて、補助記憶装置は、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵をオペレーティングシステムから取得し、その秘密鍵を用いてデータを暗号化し、暗号化したデータの転送時には暗号化したことを知らせる。オペレーティングシステムは、暗号化に必要な秘密鍵を生成し、補助記憶装置から得た公開鍵を用いて、この秘密鍵

を暗号化した後、補助記憶装置に送り、補助記憶装置からのデータの転送時に暗号化されたことを知らされた場合には、オペレーティングシステム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送り、それ以外のルーチンおよび補助記憶装置に対しては暗号化されたデータを送出するとともに暗号化されたことを知らせ、復号化に必要な秘密鍵を公開鍵暗号方式を用いて送る。又、データの書込みが可能な補助記憶装置は、暗号化されたデータの記録時に、公開鍵暗号方式を用いて受け取った秘密鍵によりデータの復号化を行ない当該データを記録メディアに記録する。

【0017】又、第6の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時に暗号化レベルを知らせることが可能な補助記憶装置と、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記補助記憶装置から得た公開鍵を用いて前記生成した秘密鍵を暗号化した後、前記補助記憶装置に送ることができ、前記補助記憶装置からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチンに対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができ、処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0018】又、第7の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時には暗号化レベルを知らせることが可能な第1の補助記憶手段と、暗号化されたデータの記録時には公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じたデータの復号化を行ない、当該データを記録メディアに記録することが可能な第2の補助記憶手段と、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記第1又は第2の補助記憶手段から得た公開鍵を用いて前記生成した秘密鍵を暗号化した後、前記第1又は第2の補助記憶手段に送ることができ、前記第1の補助記憶手段からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチン及び前記第2の補助記憶手段に対して

は暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0019】上記した第6、第7の発明によるコンピュータシステムに於いて、補助記憶装置は、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化し、暗号化したデータの転送時には暗号化レベルを知らせる。オペレーティングシステムは、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し補助記憶装置から得た公開鍵を用いてこの秘密鍵を暗号化したあと補助記憶装置に送り、補助記憶装置からのデータの転送時には暗号化レベルを取得し、オペレーティングシステム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送り、それ以外のルーチンおよび補助記憶装置に対しては暗号化されたデータと共にあらかじめ設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送る。又、データの書込みが可能な補助記憶装置は、暗号化されたデータの記録時には公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じたデータの復号化を行なって当該データを記録メディアに記録する。

【0020】又、第8の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの転送時に暗号化レベルを知らせることが可能な補助記憶装置と、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記補助記憶装置から得た公開鍵を用いて当該秘密鍵を暗号化した後、前記補助記憶装置に送ることができ、前記補助記憶装置からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチンに対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0021】又、第9の発明は、処理装置と補助記憶装置との間で複製を規制するデータが受け渡されるコンピュータシステムに於いて、公開鍵暗号化方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけ処理装置のオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じた秘密鍵を用いてデータを暗号化することが可能で、暗号化したデータの

転送時には暗号化レベルを知らせることが可能な第1の補助記憶手段と、暗号化されたデータの記録時には公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じたデータの復号化を行ない、当該データを記録メディアに記録することが可能な第2の補助記憶手段と、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し前記第1又は第2の補助記憶手段から得た公開鍵を用いて当該秘密鍵を暗号化した後、前記第1又は第2の補助記憶手段に送ることができ、前記第1の補助記憶手段からのデータの転送時には暗号化レベルを取得することができ、システム内部の出力信号処理ルーチンに対しては暗号化されたデータを復号化して送ることができ、それ以外のルーチン及び前記第2の補助記憶手段に対しては暗号化されたデータとともに予め設定されたレベルに応じた秘密鍵を公開鍵暗号方式を用いて送ることができる処理装置のオペレーティングシステムとを具備してなることを特徴とする。

【0022】上記した第8、第9の発明によるコンピュータシステムに於いて、補助記憶装置は、公開鍵暗号方式を用いてデータの暗号化に必要な秘密鍵を暗号化レベルの数だけオペレーティングシステムから取得し、保存されているデータの暗号化レベルに応じて秘密鍵を用いたデータの暗号化を複数回行ない、暗号化したデータの転送時には暗号化レベルを知らせる。オペレーティングシステムは、暗号化に必要な秘密鍵を暗号化レベルの数だけ生成し補助記憶装置から得た公開鍵を用いてこの秘密鍵を暗号化した後、補助記憶装置に送り、補助記憶装置からのデータの転送時には暗号化レベルを取得し、オペレーティングシステム内部の出力信号処理ルーチンに対しては暗号化されたデータを暗号化レベルに応じた回数だけ復号化して送り、それ以外のルーチン及び補助記憶装置に対しては暗号化されたデータを送出するとともに予め設定されたレベルに応じた数の秘密鍵を公開鍵暗号方式を用いて送る。又、データの書込みが可能な補助記憶装置は、暗号化されたデータの記録時に、公開鍵暗号方式を用いて受け取った秘密鍵によりレベルに応じた回数だけデータの復号化を行なって当該データを記録メディアに記録する。

【0023】上記したようなデータ転送時に於ける秘密鍵を用いた暗号化処理を、システム内でのパスを経由する例えば動画データ等に対して選択的に行なうことにより、所望のデータの複製を確実に防止して信頼性の高いデータ保護機能を実現できる、補助記憶装置内のデータの暗号化及び暗号化データの扱いを考慮したコンピュータシステムが提供できる。

【0024】

【発明の実施の形態】以下図面を参照して本発明の実施形態を説明する。先ず、図1乃至図3を参照して本発明の第1実施形態について説明する。図1は本発明の第1実施形態に於けるデータ暗号化方式を用いたコンピュー

タシステムの機能構成を示すブロック図である。

【0025】この第1実施形態に於けるコンピュータシステムは、補助記憶装置に記録されたサウンドを含む動画データの再生機能、及び当該データの記録機能を備えているもので、ここでは、コンピュータ本体（PC）10と、表示装置（DISP）11と、スピーカ（SP）12と、読み出し用補助記憶装置（AUX-STOR（R））13、及び書き込み用補助記憶装置（AUX-STOR（W））14等から構成される。

【0026】また、コンピュータ本体（PC）10の内部には、中央処理装置（CPU）20、主メモリ（MEM）21、表示用メモリ（VRAM）22、ディスプレイコントローラ（DISP-CONT）23、オーディオコントローラ（AUDIO-CONT）24、読み出し用補助記憶装置コントローラ（AUX-CONT（R））25、書き込み用補助記憶装置コントローラ（AUX-CONT（W））26等が設けられ、システムバス（SYS-BUS）60を経由して相互にデータ、コマンド等の転送が行なわれる。

【0027】更に、主メモリ（MEM）21には、オペレーティングシステム（OS）30、アプリケーションソフトウェア（APPL）31等が記憶されており、オペレーティングシステム（OS）30には、秘密鍵（SEC-Key）40、復号化処理ルーチン（DEC-RTN）41、出力信号処理ルーチン（OPS-RTN）42等が含まれている。

【0028】図2、及び図3はそれぞれ本発明のデータの暗号化処理の動作説明図であり、ここでは、コンピュータ本体（PC）10内のシステムバス（SYS-BUS）60を経由して受け渡される特定のデータ（例えば著作権保護を必要とする圧縮化された動画データ等）に対して、秘密鍵（SEC-Key）40を用い、再生時に暗号化処理（図2参照）を施し、記録時に復号化処理（図3参照）を施している。

【0029】ここで上記各図を参照して本発明の第1実施形態に於ける動作を説明する。コンピュータ本体（PC）10は、各種アプリケーションの実行を行なうために必要な各種の入出力装置を含んでいる。

【0030】表示装置（DISP）11は、アプリケーションなどの実行結果を表示するために用いられ、スピーカ（SP）12は、音声データを出力するために用いられる。

【0031】読み出し用補助記憶装置（AUX-STOR（R））13は、画像データ、音声（サウンド）データ等を含んだコンピュータ上で扱うことができるデータを保持し、それらのデータを読み出し用補助記憶装置コントローラ（AUX-CONT（R））25からの命令によって転送することができる。

【0032】また、データの暗号化に必要な秘密鍵（SEC-Key）40を、公開鍵暗号方式を用いて、オペ

レーティングシステム（OS）30から取得することができる。

【0033】更に読み出し用補助記憶装置（AUX-STOR（R））13は、暗号化が必要なデータに対しての転送命令を受けたときには、予め取得していた秘密鍵（SEC-Key）40を用いてデータを暗号化して転送することができ、暗号化したデータの転送時には、暗号化したことをオペレーティングシステム（OS）30に知らせてから転送を行なうことができる。

【0034】書き込み用補助記憶装置（AUX-STOR（W））14は、各種データの転送および書き込みを行なうことができる。また、データの復号化に必要な秘密鍵（SEC-Key）40を、公開鍵暗号方式を用いてオペレーティングシステム（OS）30から取得することができる。

【0035】更に書き込み用補助記憶装置（AUX-STOR（W））14は、暗号化されたデータの書き込みを要求された時には、予め取得しておいた秘密鍵（SEC-Key）40を用いてデータを復号化して書き込むことができる。

【0036】中央処理装置（CPU）20は、オペレーティングシステム（OS）30の制御によって各種のアプリケーション（APPL）31から要求された計算を行なう。

【0037】主メモリ（MEM）21は、中央処理装置（CPU）20の作業領域に供されるとともに、オペレーティングシステム（OS）30、アプリケーション（APPL）31等を一時的に保存しておくために使用されるもので、ここでは内部で予め生成された秘密鍵（SEC-Key）40を記憶する。

【0038】表示用メモリ（VRAM）22は、アプリケーション（APPL）31がオペレーティングシステム（OS）30に対して表示装置（DISP）11に表示するように要求した画面のイメージが一時的に保存される。

【0039】ディスプレイコントローラ（DISP-CONT）23は、表示用メモリ（VRAM）22に保存されているイメージを読み出して、当該データを表示装置（DISP）11が表示するのに適した信号に変換し、表示装置（DISP）11に送出する。

【0040】オーディオコントローラ（AUDIO-CONT）24は、アプリケーションソフトウェア（APPL）31がオペレーティングシステム（OS）30に対してスピーカ（SP）12から出力するように要求したデータを受け取り、スピーカ（SP）12にオーディオ信号を出力する。

【0041】読み出し用補助記憶装置コントローラ（AUX-CONT（R））25は、オペレーティングシステム（OS）30と読み出し用補助記憶装置（AUX-STOR（R））13とのデータのやり取りを仲介す

る。

【0042】書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26は、オペレーティングシステム (OS) 30と書き込み用補助記憶装置 (AUX-STOR (W)) 14とのデータのやり取りを仲介する。

【0043】オペレーティングシステム (OS) 30は、その内部に、復号化処理ルーチン (DEC-RTN) 41、及び出力信号処理ルーチン (OPS-RTN) 42等である、画像処理用モジュール、音声処理用モジュール、暗号化されたデータを復号するための復号モジュール等をもつ。

【0044】また、読み出し用補助記憶装置 (AUX-STOR (R)) 13がデータの暗号化を行なうための秘密鍵 (SEC-Key) 40を生成することができ、その秘密鍵 (SEC-Key) 40を、公開鍵暗号方式を用いて、読み出し用補助記憶装置 (AUX-STOR (R)) 13に渡すことができる。

【0045】アプリケーション (APPL) 31が読み出し用補助記憶装置 (AUX-STOR (R)) 13に保存されているデータの転送を要求してきたときには、読み出し用補助記憶装置 (AUX-STOR (R)) 13に対してデータの転送を要求する。

【0046】このとき、読み出し用補助記憶装置 (AUX-STOR (R)) 13がデータを暗号化して転送することを通知している場合には、その旨をアプリケーション (APPL) 31に知らせる。

【0047】また、アプリケーション (APPL) 31が、暗号化されていない画像データ、音声データを出力することを要求してきた場合には、データをそのまま、それぞれ表示用メモリ (VRAM) 22、オーディオコントローラ (AUDIO-CONT) 24等に転送し、又、暗号化されているデータを出力するように要求してきた場合には、復号化モジュール (復号化処理ルーチン (DEC-RTN) 41) を通してデータの復号化を行ってから当該データを表示用メモリ (VRAM) 22、オーディオコントローラ (AUDIO-CONT) 24等に転送する。

【0048】更にオペレーティングシステム (OS) 30は、アプリケーション (APPL) 31が、暗号化されていない各種データを書き込み用補助記憶装置 (AUX-STOR (W)) 14に書き込むように指示してきたときには、書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26を介し書き込み用補助記憶装置 (AUX-STOR (W)) 14に対して書き込みを指示し、又、暗号化されたデータを書き込むように指示してきたときには、公開鍵暗号方式を用いて復号化のために必要な秘密鍵 (SEC-Key) 40を渡し、その後、暗号化されたデータを転送する。

【0049】アプリケーション (APPL) 31は、こ

こでは、画像データ、音声データを扱うアプリケーションソフトウェアである。このアプリケーション (APPL) 31は、読み出し用補助記憶装置 (AUX-STOR (R)) 13からデータを取り出し、その画像データを表示装置 (DISP) 11に表示したり、音声データをスピーカ (SP) 12から再生したりすることができる。

【0050】又、データの取り出しの際には、オペレーティングシステム (OS) 30からデータが暗号化されたものであるか否かを知らされると、その旨を当該暗号化されたデータとともに保存しておき、出力の際には暗号化されているか否かを出力先に知らせる。

【0051】更にアプリケーション (APPL) 31は、データを書き込み用補助記憶装置 (AUX-STOR (W)) 14に書き込みたいときにもオペレーティングシステム (OS) 30を通して、暗号化されているかどうかをデータとともに伝達する。

【0052】秘密鍵 (SEC-Key) 40は、暗号化及び復号化に必要な鍵であり、オペレーティングシステム (OS) 30内で生成され保持される。復号化処理ルーチン (DEC-RTN) 41は暗号化されたデータを秘密鍵 (SEC-Key) 40を用いて復号化し、その復号化されたデータを出力する機能をもっている。

【0053】ここで上記構成による第1実施形態のコンピュータシステムに於ける動作をデータの流れとともに説明する。まず、読み出し用補助記憶装置 (AUX-STOR (R)) 13に記録されている暗号化の必要な動画データA、つまり、著作権の保護のために第三者に対しては公開したくないデータをコンピュータ本体 (PC) 10に接続された表示装置 (DISP) 11、及びスピーカ (SP) 12から出力する際の処理の流れについて説明する。

【0054】アプリケーション (APPL) 31は、オペレーティングシステム (OS) 30に対して、読み出し用補助記憶装置 (AUX-STOR (R)) 13に保存されている、動画データAを取り出すように要求する。

【0055】オペレーティングシステム (OS) 30は、読み出し用補助記憶装置コントローラ (AUX-CONT (R)) 25を通して読み出し用補助記憶装置 (AUX-STOR (R)) 13に保存されている動画データAを取り出すように要求する。

【0056】読み出し用補助記憶装置 (AUX-STOR (R)) 13は、要求された動画データAが暗号化の必要なデータであることを知ると、公開鍵暗号方式を用いて、オペレーティングシステム (OS) 30から動画データAの暗号化に必要な秘密鍵 (SEC-Key) 40を取得する。

【0057】具体的には、読み出し用補助記憶装置 (AUX-STOR (R)) 13の中で、図2に示すよう

に、対になる暗号化用の鍵A (Open-Key (A)) と復号化用の鍵B (Open-Key (B)) を生成し、鍵A (Open-Key (A)) をオペレーティングシステム (OS) 30に転送する。

【0058】オペレーティングシステム (OS) 30は、内部で生成した動画データ復号化用の秘密鍵 (SEC-Key) 40を上記鍵A (Open-Key (A)) を用いて暗号化 (encrypt) し、読み出し用補助記憶装置 (AUX-STOR (R)) 13に送り返す。

【0059】読み出し用補助記憶装置 (AUX-STOR (R)) 13は、暗号化された秘密鍵 (SEC-Key) 40を上記復号化用の鍵B (Open-Key (B)) を用いて復号化 (decrypt) することで、オペレーティングシステム (OS) 30内で生成したものと同一秘密鍵 (SEC-Key) 40を取得することができる。

【0060】以上のような手順が公開鍵暗号方式と呼ばれているものである。このようにして、動画データAの暗号化に必要な秘密鍵 (SEC-Key) 40を取得した読み出し用補助記憶装置 (AUX-STOR (R)) 13は、動画データAを暗号化して転送する。このとき、データが暗号化されたものであることをオペレーティングシステム (OS) 30に知らせる。

【0061】読み出し用補助記憶装置コントローラ (AUX-CONT (R)) 25を通して暗号化された動画データAを受け取ったオペレーティングシステム (OS) 30は、アプリケーション (APPL) 31にデータを転送し、そのデータが暗号化されたものであることを知らせる。

【0062】アプリケーション (APPL) 31が受け取った、暗号化された動画データAを再生するときには、当該データをオペレーティングシステム (OS) 30に対して転送して出力を依頼する。この際、データの転送と同時に、当該データが暗号化されているものであることを知らせる。

【0063】オペレーティングシステム (OS) 30は、アプリケーション (APPL) 31から転送された、暗号化された動画データAを、以前に作成し保存しておいた秘密鍵 (SEC-Key) 40を用いて復号化して、当該動画データを表示用メモリ (VRAM) 22に書き込み、音声データをオーディオコントローラ (AUDIO-CONT) 24に転送して再生を行なうように指示する。

【0064】ディスプレイコントローラ (DISP-CONT) 23は、表示用メモリ (VRAM) 22に書き込まれた画像を表示装置 (DISP) 11に表示する。オーディオコントローラ (AUDIO-CONT) 24は音声データをスピーカ (SP) 12から再生できるように加工してスピーカ (SP) 12に送出し音声を再生

する。

【0065】この際のシステムバス (SYS-BUS) 60経由による、オペレーティングシステム (OS) 30と読み出し用補助記憶装置 (AUX-STOR (R)) 13との間の暗号化処理手順を図2に示している。

【0066】以上のような処理によってデータが暗号化された後、転送され、再生の必要な時には復号化が行なわれる。次に、アプリケーション (APPL) 31が読み出し用補助記憶装置 (AUX-STOR (R)) 13から転送された動画データBを書き込み用補助記憶装置 (AUX-STOR (W)) 14に書き込む際の処理の流れを説明する。

【0067】アプリケーション (APPL) 31が暗号化されたデータを読み出し用補助記憶装置 (AUX-STOR (R)) 13から得るまでの手順は上述した動画データAを得る際の手順と同様であるので、ここではその処理の流れを省略する。

【0068】アプリケーション (APPL) 31が暗号化された動画データBをオペレーティングシステム (OS) 30に対して書き込み用補助記憶装置 (AUX-STOR (W)) 14に書き込むように指示する。

【0069】オペレーティングシステム (OS) 30は書き込み用補助記憶装置 (AUX-STOR (W)) 14がオペレーティングシステム (OS) 30が書き込みを許可した装置であることを確認した後、公開鍵暗号方式を用いて復号化に必要な秘密鍵 (SEC-Key) 40を渡す。

【0070】オペレーティングシステム (OS) 30は、秘密鍵 (SEC-Key) 40を渡した後に、暗号化された動画データBを書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26を通して書き込み用補助記憶装置 (AUX-STOR (W)) 14に転送する。この際、当該転送データが暗号化されていることを併せて通知する。

【0071】書き込み用補助記憶装置 (AUX-STOR (W)) 14は、暗号化された動画データBを、秘密鍵 (SEC-Key) 40を用いて復号化したことを記録する。

【0072】この際のシステムバス (SYS-BUS) 60経由による、オペレーティングシステム (OS) 30と書き込み用補助記憶装置 (AUX-STOR (W)) 14との間の暗号化処理手順を図3に示している。

【0073】このようにして、オペレーティングシステム (OS) 30が書き込みを許可した装置だけが、暗号化されたデータを記録することができるようになる。次に、図4を参照して、本発明の第2実施形態、及び第3実施形態を説明する。

【0074】図4はデータ暗号化方式を用いた本発明の

10

20

30

40

50

第2実施形態、及び第3実施形態によるコンピュータシステムの機能ブロック図である。このコンピュータシステムは、コンピュータ本体 (PC) 10、表示装置 (DISP) 11、スピーカ (SP) 12、読み出し用補助記憶装置 (AUX-STOR (R)) 13、書き込み用補助記憶装置 (AUX-STOR (W)) 14等から構成される。

【0075】コンピュータ本体 (PC) 10の内部には、中央処理装置 (CPU) 20、主メモリ (MEM) 21、表示用メモリ (VRAM) 22、ディスプレイコントローラ (DISP-CONT) 23、オーディオコントローラ (AUDIO-CONT) 24、読み出し用補助記憶装置コントローラ (AUX-CONT (R)) 25、書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26等が設けられる。

【0076】主メモリ (MEM) 21には、前述した第1実施形態と異なり、2種の秘密鍵 (SEC-Key (A), SEC-Key (B)) 50, 51が設けられる。即ち、この実施形態では、主メモリ (MEM) 21に、オペレーティングシステム (OS) 30、アプリケーション (APPL) 31等が記憶されており、更に、オペレーティングシステム (OS) 30には、秘密鍵A (SEC-Key (A)) 50、及び秘密鍵B (SEC-Key (B)) 51と、復号化処理ルーチンA (DEC-RTN (A)) 52、及び復号化処理ルーチンB (DEC-RTN (B)) 53が含まれている。

【0077】ここで、上記各ブロックの機能について、上述した第1実施形態と異なる部分について説明する。秘密鍵A (SEC-Key (A)) 50は、一度だけコピーすることを許したデータに対して暗号化、及び復号化を行なうために必要な秘密鍵である。

【0078】秘密鍵B (SEC-Key (B)) 51は、データをコピーすることを禁止したデータに対して暗号化、及び復号化を行なうために必要な秘密鍵である。復号化処理ルーチンA (DEC-RTN (A)) 52は、秘密鍵A (SEC-Key (A)) 50を用いてデータを復号化するルーチンである。

【0079】復号化処理ルーチンB (DEC-RTN (B)) 53は、秘密鍵B (SEC-Key (B)) 51を用いてデータを復号化するルーチンである。次に、上記図4を参照して本発明の第2実施形態に於ける動作を説明する。

【0080】先ず、アプリケーション (APPL) 31が読み出し用補助記憶装置 (AUX-STOR (R)) 13に記録されている、一度だけコピーすることを許した動画データCを扱う際の処理の流れについて説明する。尚、ここでは上述した第1実施形態との相違点についてのみ説明を行なう。

【0081】先ず、読み出し用補助記憶装置 (AUX-STOR (R)) 13がデータを暗号化する際には、保

持しているデータが一度だけコピーすることが許されたデータであるのか、コピーすることが禁止されたデータであるのかによって、使用する秘密鍵が異なるので、オペレーティングシステム (OS) 30とのやり取りで2つの秘密鍵A, B (SEC-Key (A), SEC-Key (B)) 50, 51を取得する。

【0082】受け取ったデータの属性を上記2つの秘密鍵A, B (SEC-Key (A), SEC-Key (B)) 50, 51を使い分けて、データ (ここでは動画データC) を暗号化し転送する。

【0083】この第2実施形態の場合には、データが一度だけコピーすることを許された動画データCなので、秘密鍵A (SEC-Key (A)) 50を用いて暗号化した動画データCをオペレーティングシステム (OS) 30を通してアプリケーション (APPL) 31に転送する。このデータ転送の際には、暗号化のレベルもデータとともに伝達する。

【0084】アプリケーション (APPL) 31が暗号化された動画データCを再生する時の処理は上述した第1実施形態と同様である。アプリケーション (APPL) 31が暗号化された動画データCを書き込み用補助記憶装置 (AUX-STOR (W)) 14に対して書き込む時の処理を以下に説明する。

【0085】先ず、アプリケーション (APPL) 31が保持しているデータを暗号化のレベルとともにオペレーティングシステム (OS) 30に渡し、書き込み用補助記憶装置 (AUX-STOR (W)) 14に記録するように指示する。

【0086】オペレーティングシステム (OS) 30は、データの暗号化レベルをみて、データが一度だけコピーが許されたものであることを知り、書き込み用補助記憶装置 (AUX-STOR (W)) 14に対して、秘密鍵A (SEC-Key (A)) 50を渡す。

【0087】オペレーティングシステム (OS) 30は、秘密鍵A (SEC-Key (A)) 50を渡した後に、暗号化された動画データCを書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26を通して書き込み用補助記憶装置 (AUX-STOR (W)) 14に転送する。このデータ転送の際、当該データがいずれのレベルで暗号化されているかを知らせる。

【0088】書き込み用補助記憶装置 (AUX-STOR (W)) 14は、暗号化された動画データCを秘密鍵A (SEC-Key (A)) 50を用いて復号化した後、当該データを記録する。この記録時には次回からのコピーを禁止するように動画データCの属性を記述する。

【0089】このようにして、一度だけコピーすることが許されたデータを書き込み用補助記憶装置 (AUX-STOR (W)) 14に記録することができる。次に、アプリケーション (APPL) 31が読み出し用補助記

憶装置 (AUX-STOR (R)) 13 に記録されている、コピーすることを禁止した動画データDを扱う際の処理の流れについて説明する。この場合も上述した第1実施形態との相違点についてのみ説明する。

【0090】 先ず、読み出し用補助記憶装置 (AUX-STOR (R)) 13 がデータを暗号化する際は、保持しているデータが、一度だけコピーすることが許されたデータであるのか、コピーすることが禁止されたデータであるのかによって、使用する秘密鍵が異なるので、オペレーティングシステム (OS) 30 とのやり取りで2つの秘密鍵A, B (SEC-Key (A), SEC-Key (B)) 50, 51 を取得する。

【0091】 受け取ったデータの属性を判断して、上記2つの秘密鍵A, B (SEC-Key (A), SEC-Key (B)) 50, 51 を使い分けて、データを暗号化して転送する。この実施形態の場合にはデータがコピーすることを禁止されたデータDであるので、秘密鍵B (SEC-Key (B)) 51 を用いて暗号化した動画データDをオペレーティングシステム (OS) 30 を通じてアプリケーション (APPL) 31 に転送する。このデータ転送の際には、暗号化のレベルもデータとともに送出する。

【0092】 アプリケーション (APPL) 31 が暗号化された動画データDを再生するときの処理は上述した第1実施形態と同様である。この場合には復号化に使用される秘密鍵は、秘密鍵B (SEC-Key (B)) 51 である。

【0093】 アプリケーション (APPL) 31 が暗号化された動画データDを書き込み用補助記憶装置 (AUX-STOR (W)) 14 に対して書き込もうとしたときには以下のような処理により書き込むことが出来なくなっている。

【0094】 先ず、アプリケーション (APPL) 31 が保持しているデータを暗号化のレベルとともにオペレーティングシステム (OS) 30 に渡し、書き込み用補助記憶装置 (AUX-STOR (W)) 14 に記録するように指示する。

【0095】 オペレーティングシステム (OS) 30 は、データの暗号化レベルをみて、データがコピーを禁止されたものであることを知り、書き込みを拒否する。この際、アプリケーション (APPL) 31 が暗号化のレベルを偽って書き込むように指示したとしても、オペレーティングシステム (OS) 30 が書き込み用補助記憶装置 (AUX-STOR (W)) 14 に対して伝達する秘密鍵は、秘密鍵A (SEC-Key (A)) 50 なので復号化することはできない。

【0096】 以上のような処理によって、暗号化にレベルをつけてデータを不正コピーから守ることができる。次に、本発明の第3実施形態の動作を上記図4を参照してデータの流れとともに説明する。

【0097】 先ず、アプリケーション (APPL) 31 が読み出し用補助記憶装置 (AUX-STOR (R)) 13 に記録されている、一度だけコピーすることを許した動画データCを扱う際の処理の流れについて説明する。尚、ここでは第1実施形態との相違点についてのみ説明する。

【0098】 先ず、読み出し用補助記憶装置 (AUX-STOR (R)) 13 がデータを暗号化する際には、保持しているデータが一度だけコピーすることが許されたデータであるのか、コピーすることが禁止されたデータであるのかによって、使用する秘密鍵が異なるので、オペレーティングシステム (OS) 30 とのやり取りで2つの秘密鍵A, B (SEC-Key (A), SEC-Key (B)) 50, 51 を取得する。

【0099】 受け取ったデータの属性を判断して、一度だけコピーすることが許されたデータの場合には、秘密鍵A (SEC-Key (A)) 50 だけを用いた暗号化を行なう。又、コピーすることが禁止されたデータの場合には、秘密鍵B (SEC-Key (B)) 51 を用いた暗号化のあとに、更に秘密鍵A (SEC-Key (A)) 50 を用いた暗号化を行なう。

【0100】 この場合には、データが一度だけコピーすることが許されたデータなので、秘密鍵A (SEC-Key (A)) 50 を用いて暗号化した動画データBをオペレーティングシステム (OS) 30 を通じてアプリケーション (APPL) 31 に転送する。このデータ転送の際には、暗号化のレベルも当該データとともに伝達する。

【0101】 アプリケーション (APPL) 31 が暗号化された動画データCを再生する時の処理は上述した第1実施形態と同様である。アプリケーション (APPL) 31 が暗号化された動画データCを書き込み用補助記憶装置 (AUX-STOR (W)) 14 に対して書き込む時の処理を以下に説明する。

【0102】 先ず、アプリケーション (APPL) 31 が保持しているデータを暗号化のレベルとともにオペレーティングシステム (OS) 30 に渡し、書き込み用補助記憶装置 (AUX-STOR (W)) 14 に記録するように指示する。

【0103】 オペレーティングシステム (OS) 30 は、データの暗号化レベルをみて、データが一度だけコピーが許されたものであることを知り、書き込み用補助記憶装置 (AUX-STOR (W)) 14 に対して秘密鍵A (SEC-Key (A)) 50 を伝達する。

【0104】 オペレーティングシステム (OS) 30 は、秘密鍵A (SEC-Key (A)) 50 を渡した後に、暗号化された動画データCを書き込み用補助記憶装置コントローラ (AUX-CONT (W)) 26 を通じて書き込み用補助記憶装置 (AUX-STOR (W)) 14 に転送する。この際、当該データがいずれのレベル

で暗号化されているかを知らせる。

【0105】書き込み用補助記憶装置(AUX-STOR(W))14は、暗号化された動画データCを、秘密鍵A(SEC-Key(A))50を用いて復号化した後、当該データを記録する。この記録時には、次回からのコピーを禁止するように動画データCの属性を記述する。

【0106】このようにして一度だけコピーすることが許されたデータを書き込み用補助記憶装置(AUX-STOR(W))14に記録することができる。次に、アプリケーション(APPL)31が読み出し用補助記憶装置(AUX-STOR(R))13に記録されている、コピーすることを禁止した動画データDを扱う際の処理の流れについて説明する。この場合も上述した第1実施形態との相違点についてのみ説明する。

【0107】先ず、読み出し用補助記憶装置(AUX-STOR(R))13がデータを暗号化する際には、保持しているデータが、一度だけコピーすることが許されたデータであるのか、コピーすることが禁止されたデータであるのかによって、使用する秘密鍵が異なるので、オペレーティングシステム(OS)30とのやり取りで2つの秘密鍵A、B(SEC-Key(A)、SEC-Key(B))50、51を取得する。

【0108】この動作例の場合にはデータがコピーすることを禁止されたデータなので、動画データDを秘密鍵B(SEC-Key(B))51を用いて暗号化し、更に秘密鍵A(SEC-Key(A))50を用いて暗号化した後、オペレーティングシステム(OS)30を通してアプリケーション(APPL)31に転送する。このデータ転送の際には、暗号化のレベルも当該データとともに伝達する。

【0109】アプリケーション(APPL)31が暗号化された動画データDを再生するときは、データのレベルをみて、秘密鍵A(SEC-Key(A))50による復号化だけか、もしくは、秘密鍵A(SEC-Key(A))50による復号化と秘密鍵B(SEC-Key(B))51による復号化の2段階の復号化を行なった後にデータを出力する。この動作例の場合には2段階の復号化が行なわれる。

【0110】アプリケーション(APPL)31が暗号化された動画データDを書き込み用補助記憶装置(AUX-STOR(W))14に対して書き込もうとしたときには、以下のような処理により書き込むことができなくなっている。

【0111】先ず、アプリケーション(APPL)31が保持しているデータを暗号化のレベルとともにオペレーティングシステム(OS)30に渡し、書き込み用補助記憶装置(AUX-STOR(W))14に記録するように指示する。

【0112】オペレーティングシステム(OS)30

は、データの暗号化レベルをみて、データがコピーを禁止されたものであることを知り、書き込みを拒否する。この際、アプリケーション(APPL)31が暗号化のレベルを偽って書き込むように指示したとしても、オペレーティングシステム(OS)30が書き込み用補助記憶装置(AUX-STOR(W))14に対して伝達する秘密鍵は、秘密鍵A(SEC-Key(A))50であるのでデータを復号化することはできない。

【0113】以上のような処理によって、暗号化にレベルをつけてデータを不正コピーから守ることができる。また、この実施の形態では、コピー禁止のデータに対して2段階暗号化を行なうので第2実施形態よりデータコピーに対する安全性が向上する。

【0114】なお、本発明は上記した実施の形態に限定されるものではない。例えば、扱うデータは動画データだけではなく、画像だけのデータでも音声だけのデータでもよいし、ここで示した以外のデータであってもよい。

【0115】また、上記した実施形態では、補助記憶を読み出し用補助記憶装置(AUX-STOR(R))13と、書き込み用補助記憶装置(AUX-STOR(W))14とを別体で設けた構成としているが、読み込み用補助装置と、書き込み用補助装置とが同一の装置であってもよい。例えば書き替え型DVDを記録媒体とする単一のドライブ装置であってもよい。

【0116】更に、暗号化のレベルも2つではなく、3つ以上のレベルに分けて暗号化を行なってもよい。また、システム構成等も本発明の要旨を逸脱しない範囲で種々変形して実施することが可能である。

【0117】以上のように本発明の実施形態によれば、補助記憶装置とオペレーティングシステムとの間で秘密鍵を用いてデータを暗号化して転送することが可能である。更に、オペレーティングシステムがデータを出力装置に出力するまで暗号化したまま保持することにより、同一コンピュータ上でさえもデータを保護することが可能となる。また、データの機密レベルに応じた暗号化が可能となる。

【0118】このような実施形態の機能をもつことにより、コンピュータシステム上に於ける補助記憶装置とオペレーティングシステムとの間に於ける転送データについても有効な暗号化処理を施し複製を確実に防止して信頼性の高いデータ保護機能を実現できる。

【0119】また、上記したようなデータ転送時に於ける秘密鍵を用いた暗号化処理を、システム内でのバスを経由する例えば動画データ等に対して選択的に行なうことにより、所望のデータの複製を確実に防止して信頼性の高いデータ保護機能を実現できる、補助記憶装置内のデータの暗号化及び暗号化データの扱いを考慮したコンピュータシステムが提供できる。

【0120】

【発明の効果】以上のように本発明によれば、補助記憶装置とオペレーティングシステムとの間でデータを暗号化して転送することが可能である。さらに、オペレーティングシステムがデータを出力装置に出力するまで暗号化したまま保持することにより、同一コンピュータ上でさえもデータを保護することが可能となる。また、データの機密レベルに応じた暗号化が可能となる。更に、上記したようなデータ転送時に於ける秘密鍵を用いた暗号化処理を、システム内でのバスを経由する例えば動画データ等に対して選択的に行なうことにより、所望のデータの複製を確実に防止して信頼性の高いデータ保護機能を実現できる。補助記憶装置内のデータの暗号化及び暗号化データの扱いを考慮したコンピュータシステムが提供できる。

【図面の簡単な説明】

【図1】本発明の第1実施形態に於けるシステムの機能構成を示すブロック図。

【図2】上記第1実施形態に於ける、システムバス (SYS-BUS) 60 経由による、オペレーティングシステム (OS) 30 と読み出し用補助記憶装置 (AUX-STOR (R)) 13 との間の暗号化処理手順を示す動作説明図。

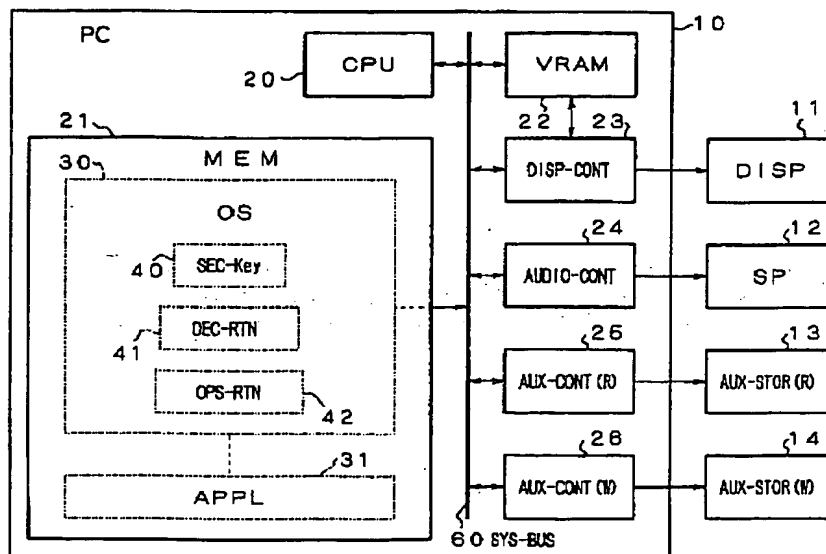
【図3】上記第1実施形態に於ける、システムバス (SYS-BUS) 60 経由による、オペレーティングシステム (OS) 30 と書き込み用補助記憶装置 (AUX-STOR (W)) 14 との間の暗号化処理手順を示す動作説明図。

【図4】本発明の第2実施形態、及び第3実施形態に於けるシステムの機能構成を示すブロック図。

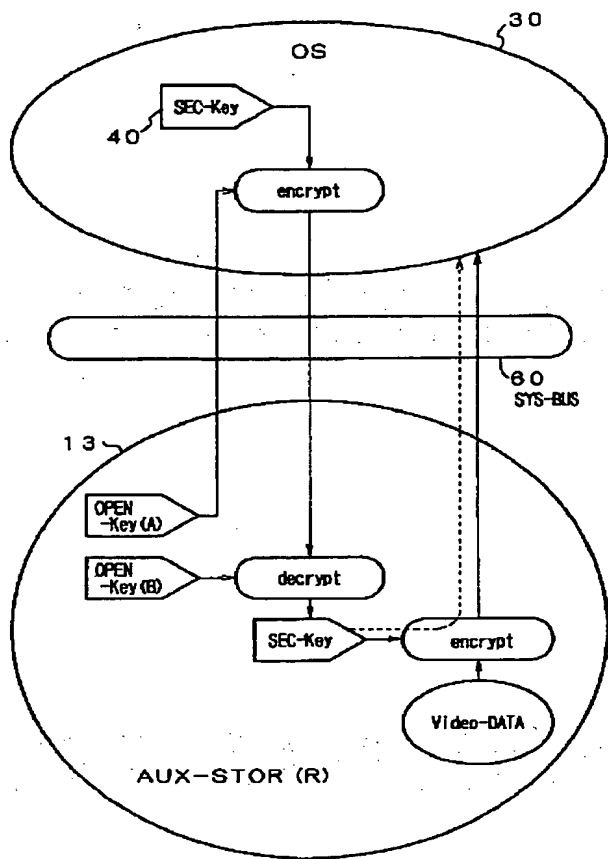
【符号の説明】

- 10…コンピュータ本体 (PC)、
- 11…表示装置 (DISP)、
- 12…スピーカ (SP)、
- 13…読み出し用補助記憶装置 (AUX-STOR (R))、
- 14…書き込み用補助記憶装置 (AUX-STOR (W))、
- 20…中央処理装置 (CPU)、
- 21…主メモリ (MEM)、
- 22…表示用メモリ (VRAM)、
- 23…ディスプレイコントローラ (DISP-CONT)、
- 24…オーディオコントローラ (AUDIO-CONT)、
- 25…読み出し用補助記憶装置コントローラ (AUX-CONT (R))、
- 26…書き込み用補助記憶装置コントローラ (AUX-CONT (W))、
- 30…オペレーティングシステム (OS)、
- 31…アプリケーション (APPL)、
- 40…秘密鍵 (SEC-Key)、
- 41…復号化処理ルーチン (DEC-RTN)、
- 42…出力信号処理ルーチン (OPS-RTN)、
- 50…秘密鍵A (SEC-Key (A))、
- 51…秘密鍵B (SEC-Key (B))、
- 52…復号化処理ルーチンA (DEC-RTN (A))、
- 53…復号化処理ルーチンB (DEC-RTN (B))、
- 60…システムバス (SYS-BUS)。

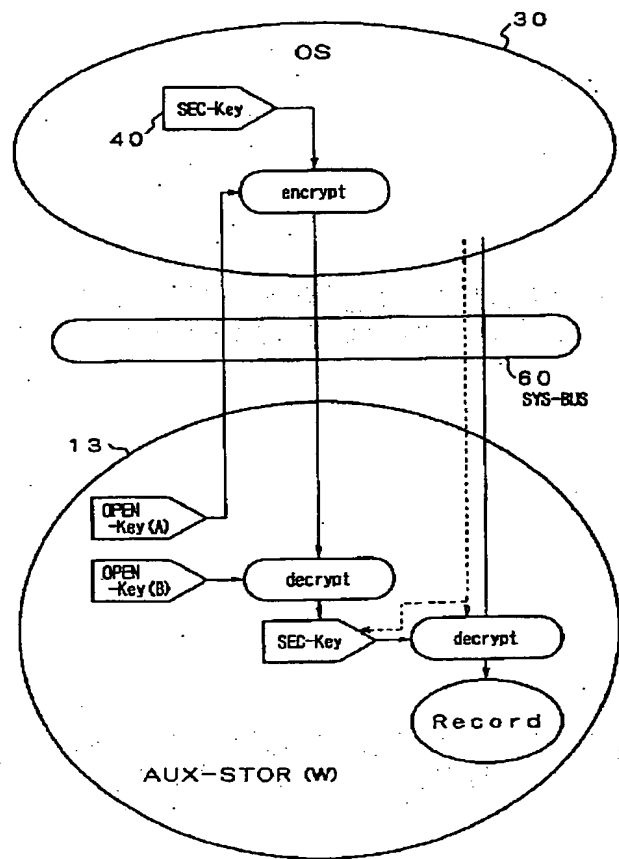
【図1】



【図2】



【図3】



【図4】

